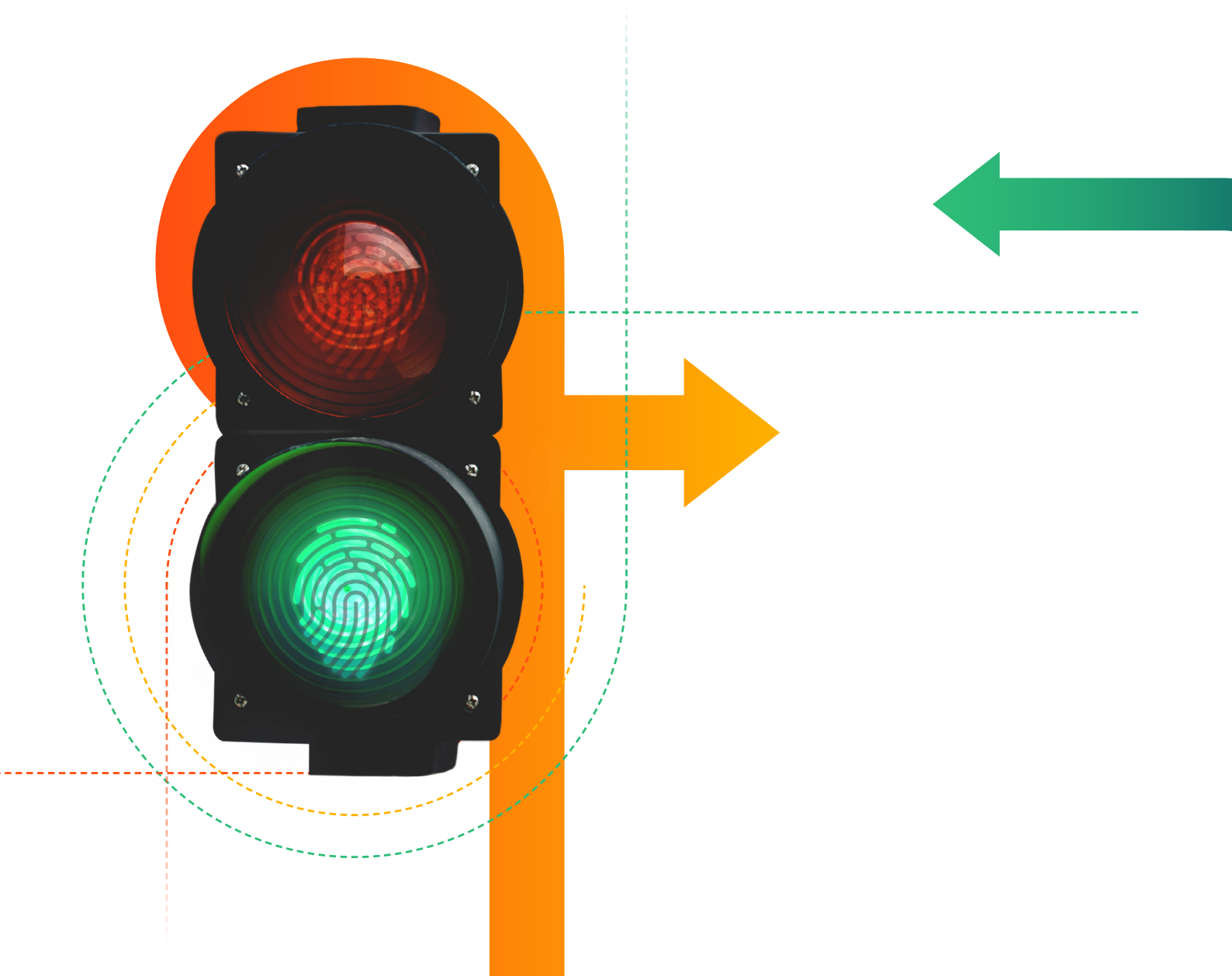
The CISO Circuit by
YL VENTURES

Top CISO Insights Edition 6

Identity & Access Management



About YL Ventures

YL Ventures funds and supports Israeli tech entrepreneurs from seed to lead. Based in Silicon Valley and Tel Aviv, the firm currently manages over $300 million and exclusively invests in cybersecurity.

YL Ventures is uniquely focused on supporting the U.S. go-to-market of early stage companies and leverages a vast network of industry experts, CISOs and U.S.-based technology companies as advisors, prospective customers and acquirers of its portfolio businesses. The fund's focused strategy allows it to conduct rapid and efficient evaluations for early stage entrepreneurs and guide founders through their ideation processes pre-investment. The fund is also dedicated to providing unmatched hands-on value-add support to each of its portfolio companies, both strategically and tactically, across multiple functions post-investment.

The firm's global network and footing in the U.S. have always counted among its most powerful assets: YL Ventures bridges the gap between Israeli innovation and the U.S. market. The firm has formalized and amplified this core competitive advantage through the launch of YL Ventures' Venture Advisory Board.

YL Ventures' Venture Advisory Board is composed of over 90 security professionals from leading multinationals, including Microsoft, Intuit, Zscaler, Kraft Heinz, Walmart, Netflix, Nike, Google, Aetna and Optiv. The firm's relationship with its advisors, as well as its extended network, is symbiotic in nature: the advisors bolster the YL Ventures investment due diligence process and provide the firm's portfolio companies continuous support across a multitude of functions throughout their life cycles; In return, network members benefit from introductions to pre-vetted Israeli cybersecurity innovations and receive direct exposure to a market second only to the U.S. in cybersecurity innovation.

Portfolio

grip
SaaS Security Management
www.grip.security

build.security
Authorization Policy Management
www.build.security

enso
Application Security Management
www.enso.security

satori
Secure Data Access Cloud
www.satoricyber.com

cycode
Source Code Control, Detection & Response Platform
www.cycode.com

orca security
Full Stack Cloud Visibility Platform
www.orca.security

Hunters.
Knowledge-Powered XDR
www.hunters.ai

VULCAN.
Continuous Vulnerability Remediation Platform
www.vulcan.io

MEDIGATE
Medical IoT Security and Asset Management
www.medigate.io

Karamba Security
Embedded Security for Connected Systems
www.karambasecurity.com

RIDEVISION
Predictive Vision for Motorcycles
www.ride.vision

Acquisitions

AXONIUS
Exited to late-stage investors

Twistlock
Acquired by paloalto

HEXADITE
Acquired by Microsoft

FIRELAYERS
Acquired by proofpoint

Seculert
Acquired by radware

BlazeMeter
Acquired by ca technologies

Clicktale
Exited to Amadeus Capital Partners

AccelaWeb
Acquired by Limelight Networks

UPSTREAM COMMERCE
Acquired by Walmart

About the CISO Circuit

YL Ventures frequently confers with an extended network of prominent cybersecurity professionals, including our Venture Advisory Board and industry executives, to assess our portfolio prospects, inform market predictions and cultivate portfolio company business development. As such, we have established direct lines of communication with the global market's preeminent CISOs and cybersecurity experts for ongoing insights into their thoughts, priorities and opinions about the state of their organizational cybersecurity.

We recognize the value this information presents to entrepreneurs, especially those wishing to enter the U.S. cybersecurity market, and to the cybersecurity community as a whole. For this reason, YL Ventures launched 'The CISO Circuit', an initiative under which we publish reports containing gathered intelligence for general use.

We hope the observations compiled in this report will prove a useful resource for aspiring cybersecurity entrepreneurs and the rest of the cybersecurity community.

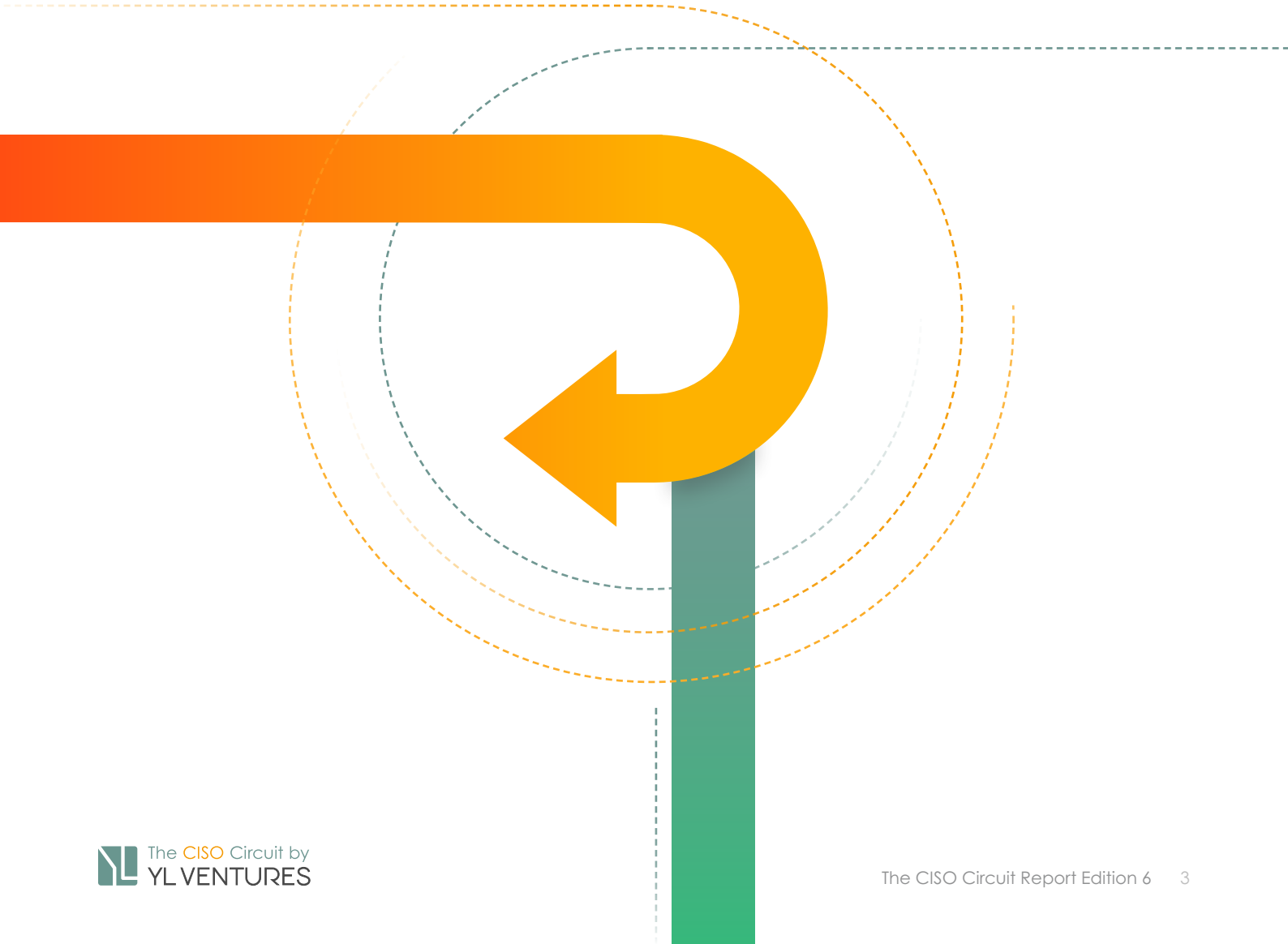


Table of Contents

Introduction

This document constitutes the sixth edition of the CISO Circuit report and contains data gathered from direct interviews with 40 cybersecurity executives at leading enterprises from YL Ventures' Venture Advisory Board. The surveys consisted of short-form questionnaires and longer-form discussion. In order to obtain the most candid data possible, and with respect to the sensitive nature of some of the information shared, we anonymized the names of our respondents and their associated organizations.

In this report, our research team set out to understand the cybersecurity challenges posed by identity and access management (IAM) in enterprise security. Over the course of 40 interviews with distinguished survey participants hailing from a diverse spectrum of verticals and company sizes, we collected responses to a series of questions (see Appendix) to their most pressing IAM needs and concerns.

The number of identities requiring management is exponentially increasing. Not only is there a growing number of users including employees, contractors, suppliers, and vendors, who all need access to corporate assets, but there is also a growing need to secure non-user identities – for example, applications that also have identities. Furthermore, there's an increasing number of assets to which secure access is required. Increasingly, individuals within enterprises at various levels need access to different cloud infrastructures, SaaS applications, and connected devices.

Identity and access management has been long underserved by the cybersecurity market. Despite its function as an elementary enterprise security practice, IAM's technology has failed to keep pace with concerted user demands. Many of today's IAM solutions are anchored in a world where companies have a single, well-defined perimeter to protect and passwords are considered adequate to maintain security. Moreover, IAM products are often still too intertwined with enterprise IT departments that are primarily focused on access and performance for their employees and lack context around security realities from potential attackers' point of view. As a result, many existing IAM tools have failed to fulfill the needs of today's enterprises.

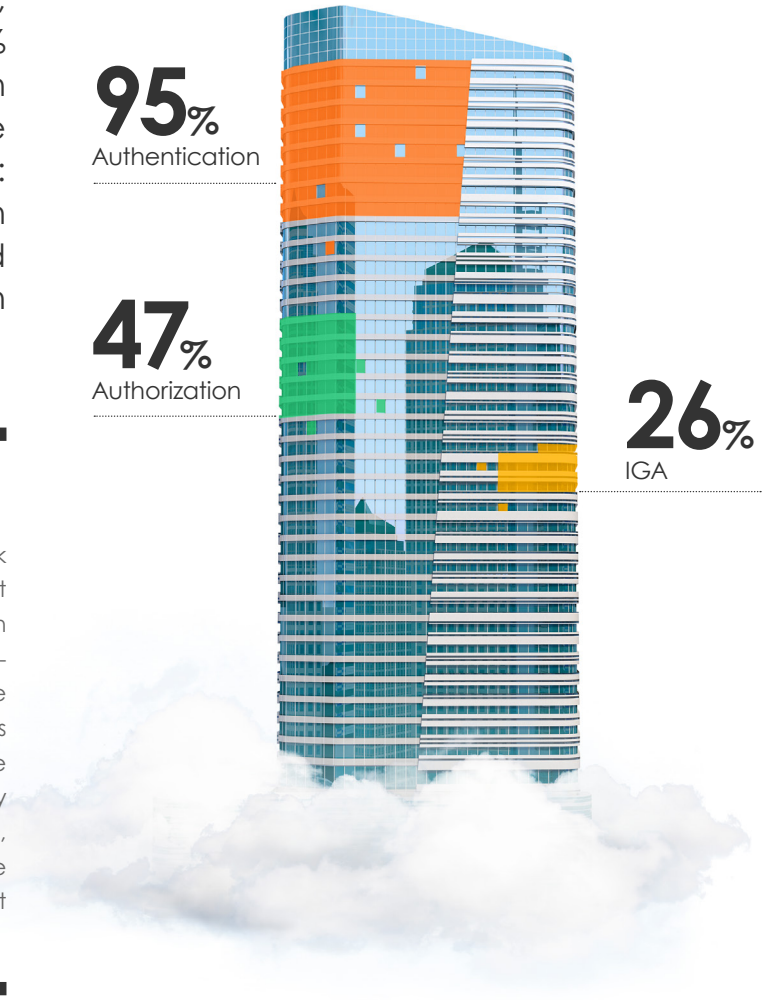
Another major obstacle is that IAM projects are often lengthy, expensive and cumbersome, making them challenging to implement and difficult to get buy-in from management. Part of this resistance is related to the potential for added friction to existing authentication and/or authorization processes, particularly those that apply directly to daily workflow. Our respondents noted that today these problems are not being addressed holistically and the ongoing reliance on point solutions has left many users dependent on managing integrations.

These phenomena raise the need for a central and single source of truth for IAM, providing visibility and management of all the identities and all assets to which these identities need to access.

The State of Enterprise IAM

The overwhelming majority (95%) of the enterprise security experts surveyed for this report use authentication as their primary means of managed identity and access, while 47% rely on authorization and 26% on identity governance & administration (IGA) providers. These findings reflect the critical missions built into IAM system design: determining who gets access, what can be accomplished with that access, and how identities are governed within an organization.

Most used IAM tools



Authentication & Authorization

Authentication mechanisms are the basic building block of any security program, and in a previous CISO Circuit edition, we outlined that their importance is also evident in the prevalence of Single Sign On (SSO) related to Software-as-a-Service (SaaS) security [1]. But authentication is just the first step in instituting enterprise security. Once the user's identity has been verified, how can leadership ensure they have access only to the specific assets which they need? This functionality is a rising challenge facing IAM, and as a result, a number of authentication providers are starting to branch out into authorization services, but not always successfully.

Identity Governance & Administration (IGA)

IGA providers help enterprises to govern their user identities and access control within the organization. Using a policy-based approach, IGAs combine identity governance and administration to support the auditing and meeting of compliance requirements. Traditionally, IGA vendors would govern identities in the form of human users, and mostly in traditional on-premise and closed perimeter environments, but changes to the nature of work and remote access are presenting new challenges to organizations when it comes to identity governance.

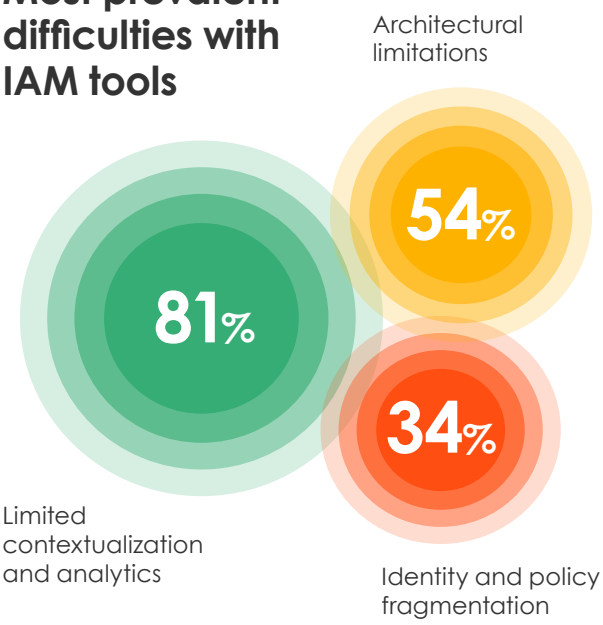
These findings reflect the critical missions built into IAM system design: determining who gets access, what can be accomplished with that access, and how identities are governed within an organization.

[1] For further reference, see SaaS Security -The CISO Circuit Edition 5

Challenges with IAM Tools

Of all the challenges inherent in today's IAM management tools, respondents pointed to their limited ability to offer contextualization and analytics as the most pressing challenge (81%), followed by their architectural limitations (54%) and the fact that they often lead to identity and policy fragmentation (34%). The fundamental shortcoming of identity fragmentation is caused by the limited contextualization and architectural limitations of today's tools.

Most prevalent difficulties with IAM tools



Limited Contextualization and Analytics

In most enterprises, users, tend to accumulate more and more access over the years irrespective of the changing roles and ensuing needs. However, this access is rarely taken back once it is extended. As IT and security teams lack contextual understanding around whether access is needed for a user or not, managers are forced to control what their direct reports can access on a case by case basis. However, this also breaks the context chain, as managers often don't understand the overall impact of the access they are granting on an organization-wide scale.

Given that the integration between Human Resources and IAM systems is often tenuous, frequent organizational changes turn access approval into an ongoing process that occurs frequently. Further, IAM systems focused on authentication rely on implicit trust for extended periods of time until that user logs out, instead of constant verification. As a result, this lack of context floods User and Entity Behavior Analytics (UEBA) systems with false positives and leads to incomplete reporting and approval flows that cause more problems than they solve.

Architectural Limitations

IAM solutions are ultimately as good as the strength of their integrations. A single solution would require authentication mechanisms to interact directly with authorization platforms and other tools, as well as with different parts of the business. This also includes physical hardware, Mac and Windows operating systems, SaaS tools, cloud platforms and more, making it impractical for a single enterprise to dedicate dozens of engineers just to IAM in order to ensure all of these different systems communicate with each other. Surveyed experts contending with hybrid environments are burdened by their reliance on the Active Directory and other legacy solutions, making their IAM processes for cloud environments more cumbersome than productive.

According to our survey respondents, IGA providers are increasingly reinvigorating their products to align with modern environments and emerging technologies, however, many are still tied to a single tenant SaaS model instead of a multi-tenant model, which limits their applicability, particularly in SaaS applications. Case in point: IAM customer agreements increasingly include non-aggregation clauses in order to prevent the commingling of data belonging to several different customers. This is challenging to enforce in multi-tenant SaaS across multiple datastores where the only logical separation of customer data is by account ID.

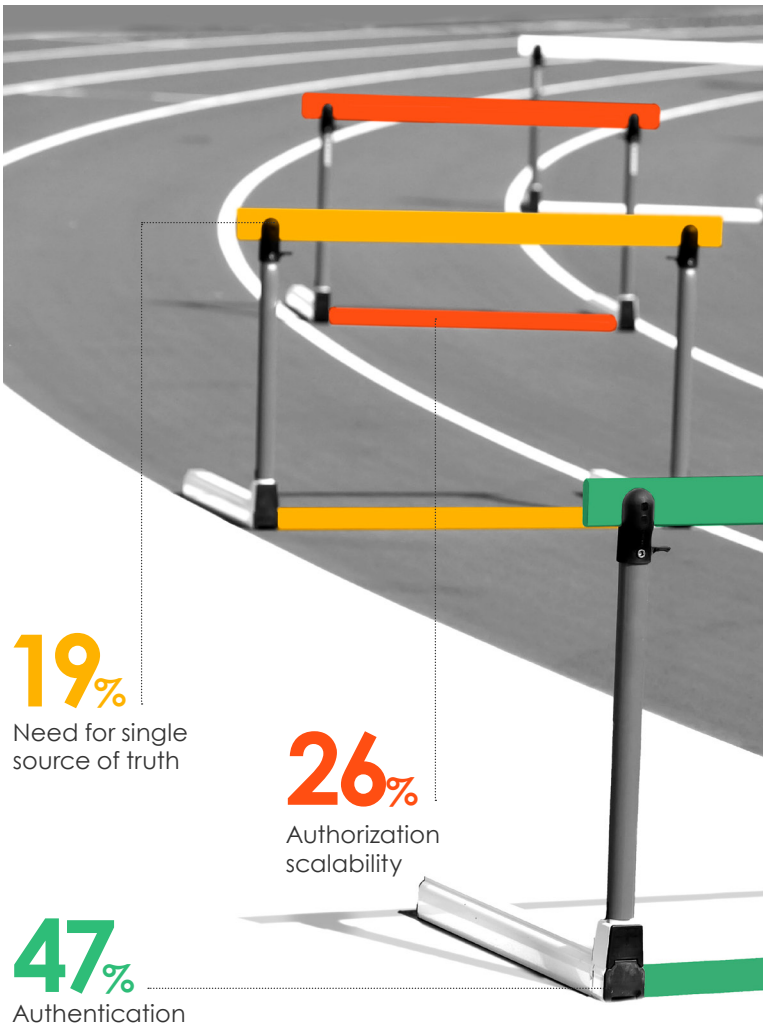
Identity and Policy Fragmentation

Transitive identity is a growing problem in our increasingly transactional workforce. In the case of freelancers or project-based contractors, access might be granted for a few weeks or months at a time, long enough to cover the job that needs to be done, but if that user returns to that same organization for an additional short-term hiring, the process must be initiated again from scratch. IAM platforms treat their identities and ensuing permissions as if their previous engagement didn't occur and so they have inadequate permissions, since their identity is not transitive nor transferable between the places they work. A further byproduct of the transactional workforce phenomenon from a security perspective is a sprawl of identities with corporate permissions on shadow IT, with users forced to work on personal laptops or devices instead of secure, company-controlled hardware.

Security teams ultimately have to contend with a multitude of identities, the number and variety of which is continuously increasing. To make matters worse, they also face growth in the number and variety of assets with which these identities must receive various forms of access. Today's engineers are searching for means to manage IAM on their own, without tools, using configuration-as-code. However, IAM roles generated through infrastructure-as-code environments such as Terraform are hardly sufficient stand-ins as they provide insufficient automated rule-based approvals, and limited time-based approvals, access reviews and compliance.

Emerging Challenges for IAM

Among the IAM challenges that our survey respondents expect to see in the near future, authentication scalability concerns (47%) were the most prevalent, followed by questions surrounding authorization scalability (26%) and the extant lack of a single source of truth for all enterprise identities and access requests (19%).

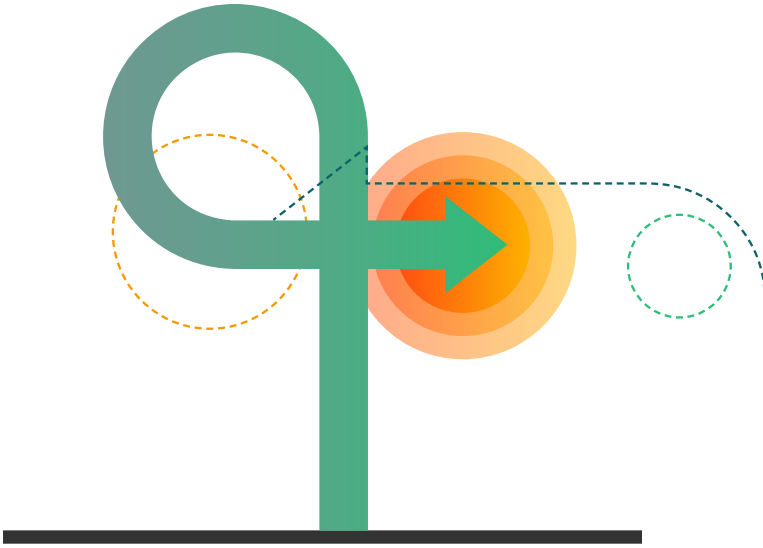


Authentication Scalability

The challenges around authentication scalability are related to how difficult it is to model for various identities, which access rights go by default to which role. Part of the problem is due to the fact that identity is typically tied to a specific individual, whereas in recent years, there has been an immense increase in device or application identities. The growth of Secure Access Service Edge (SASE) and Cloud Access Security Broker (CASB) systems have only exacerbated this problem, creating a mix of on-premise, SaaS and third-party platforms that don't always integrate with IAM systems.

According to our respondents, a new solution is needed that can define and manage identities "up and down the stack," addressing each user's identity across platforms ranging from cloud infrastructure, to SaaS services, to mobile VPNs and more. Security teams should be able to manage identities across all applications regardless of the third-party tool they're using.

Security teams should be able to manage identities across all applications regardless of the third-party tool they're using.



Authorization Expansion

After access, scaling authorization systems is the second-largest IAM challenge that enterprise respondents see on the horizon, in part because of the disconnect that currently exists between both steps in many IAM systems. The majority of companies today attempt to remedy the authorization problem using technology alone, but doing so is insufficient as it neglects the core principles behind the practice and process that goes into identity management.

Zero trust systems, in particular, can be difficult to scale since they typically begin with identities before analyzing the device which identities need access to, and its security. Respondents stated that as a result, they are often left to verify that every connection is made properly and that data is flowing, complicating what should be an automatic process and presenting roadblocks to true scale.

For instance, while systems that include granular permissions settings might seem desirable, the end result is an authorization map that includes thousands of different combination possibilities that further complicates permission setting.

The Search for a Single 'Source of Truth'

The scale of companies' security needs evolves as they grow and as they introduce structural changes. This change oftentimes takes place during mergers and acquisitions, or simply when increased growth leads to the addition of more SaaS applications, presenting new challenges for IAM providers. The addition of new applications necessitates a single source of truth for identity and access management, due to the growing utilization of freelancers and contract or project-based employees, requiring additional access demands.

The push for this single source of truth boils down to simplicity. Today's platforms are too fragmented and specific, requiring users to juggle multiple products to accomplish their goals rather than rely on one that can do everything. Users at all levels are impacted by IAM controls, and every step in the process increases friction and threatens adoption. A single source of truth solution can reduce complexity while also cutting down on end user friction. That said, adoption hinges on user friendliness and ease of use. CISOs who are looking for easy wins in IAM strategy should prioritize usability and simplicity over security alone, as seamless and frictionless solutions tend to be the most popular and widely adopted.

Opportunities in Enterprise IAM

Looking ahead, respondents see many opportunities for IAM to adapt to changing market demands by embracing new approaches to privileged access, developer tools, centralization and automation, granular access and password management.

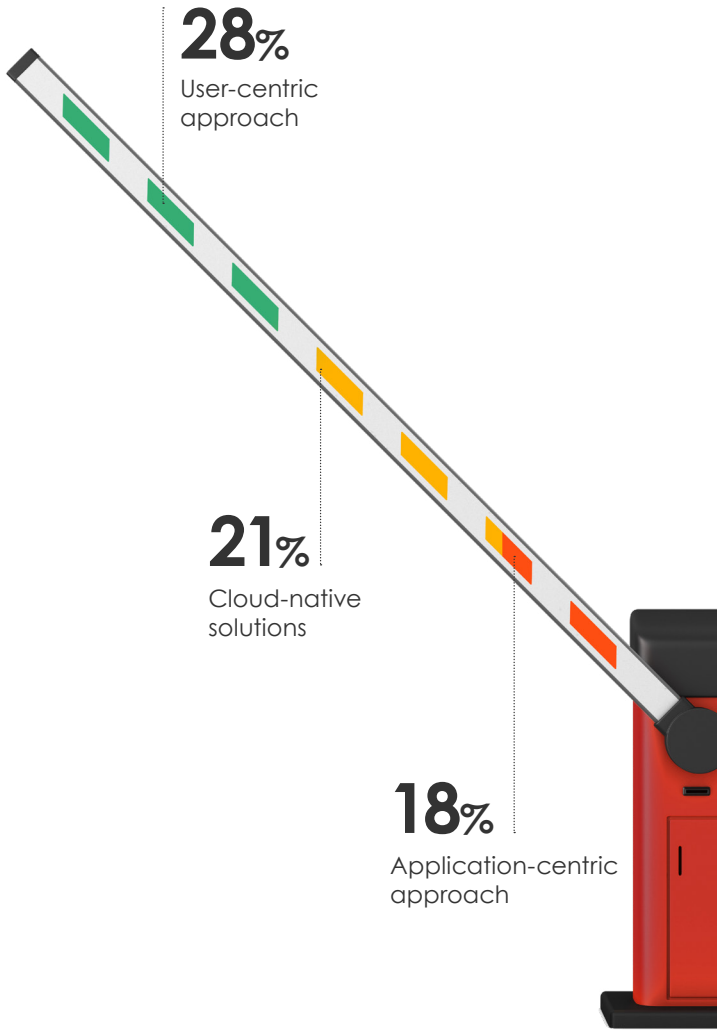
Privileged Access

In many enterprises, privileged access management (PAM) frequently triggers inter-organizational power struggles between engineering, security, and IT teams. Numerous secrets are hard coded in scripts and systems, and retrofitting legacy systems to use vaults is extremely difficult. The use of the same username and password for all service accounts, rendering them as having "god-level access" occurs often and rarely changes due to the concern that something may break. 28% of respondents prefer a user-centric approach, whereas 21% prefer cloud-native solutions and 18% an application-centric approach.

The user-centric approach metes out privileged access to specific assets per identity, and is the most utilized PAM strategy by today's enterprises. Some respondents reported being concerned about storing credentials for third party systems as well as dealing with outsourced workers, which might leave credentials at risk. Cloud-native solutions, on the other hand, typically rely on just-in-time (JIT) permissions which allow for temporary access on a project-by-project basis. Companies with traditional PAMs can protect their keys for these permissions behind a firewall, but key management can become a problem when dealing with outside providers and others not within the company's perimeter.

An application-centric approach shifts attention to the application and even to the data layer, defining and implementing how access should be provisioned based on the type of application to which access is requested. The challenge with this approach is when companies are dealing with thousands of service and administrative accounts as there is currently a limit on how many of these accounts can be paired with domain administrators.

How should privileged access be managed?

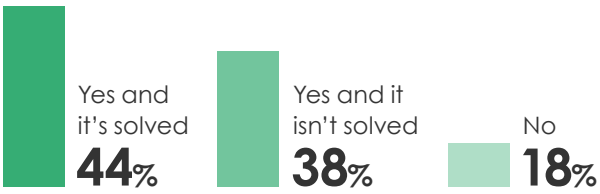


Some respondents reported being concerned about storing credentials for third party systems as well as dealing with outsourced workers, which might leave credentials at risk.

Developer Access to Production Environments

The majority of respondents said that developer access to production environments is a priority, but there remains some differentiation between those who have implemented solutions to the challenge (44%), and those who have not yet implemented methodologies to address the issue (38%). 18% said that developer access was not a priority at this point.

Is developer access to production environments a priority?



Developer access to production environments has been addressed in a myriad of ways. Dedicated SSOs and the PAMs used by the three main cloud providers (AWS, GCP, Azure), are common solutions, in combination with internal workflows. Most respondents employ a complete limitation of developer access to the production environment.

However, the default policy for some enterprises is to lock developers out of production environments once their code is deployed. At that point, the responsibility moves to the operations team. The reason for this is that the more developers there are in production, the less stable the platform becomes.

However, the more agile the development process is, the less sustainable these silos become. Sometimes developers need more ready access than they have traditionally enjoyed. Some respondents have built custom solutions to check in and out of access, as there are almost no commodity solutions that address developer access in production environments, while others rely on internal processes to review access in retrospect. But there remains potential for innovation here, including in automation to temporarily grant new privileges in response to access denied audit events, as well the option to instantly revoke them. Some organizations may find the increased risk from such a solution an acceptable tradeoff for the enhanced speed and flexibility that comes with automation.

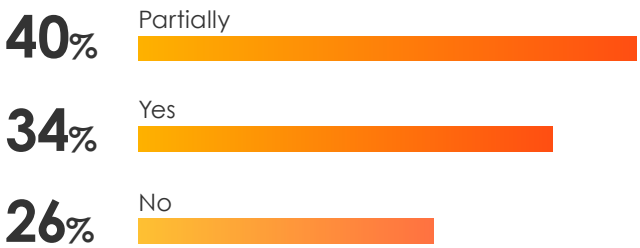
Centralizing Access Provisioning

The centralization and automation of access provisioning remains a work in progress, with only 34% of respondents reporting that they had completed the process, 40% had partially implemented and 26% had not yet begun the process.

Among those that had, some centralized the onboarding process by building different systems for creating new accounts, while others leveraged custom orchestration engines, or simply documented all of the applications involved with each identity in order to overcome the complexity of centralized access provisioning.

Some advisers have account provisioning created from a combination of home-grown IAM tools to centralize access for SaaS or IaaS access. The tools entail access packages that are attached to business roles, providing centralized management to grant necessary access rights to everyday work. Another solution mentioned by advisers is enabling centralized access verification in which security teams can go back to the target system to understand which access rights were implemented and reconcile it with the business needs of certain roles. However, the time invested to review, audit, and assess permissions under this type of system can be problematic.

Have you centralized and/or automated access provisioning?



Additional Granular Access Controls

Just over half of respondents (52%) have implemented granular access controls within their IAM systems, while 48% have not, for a variety of reasons.

While being able to leverage more granular access controls is a positive for most users, their inclusion in IAM today comes with a tradeoff. These types of options are typically dependent on the service or application involved – not all support custom controls – and can often add to the overall cost of implementation. Solutions that aim to provide this functionality, such as Slack Grid for example, charge a significant premium for this added capability. Still, there is demand for customer-specific access for limited periods of time in production data stores, data warehouses, and to major SaaS services such as Salesforce, as well as to provide access transparency based on support tickets or assignments created within Salesforce.

Conversely, some of our respondents prefer to stick with the controls that their IAM platform offers and accept whatever security risk that comes with it, rather than push for custom options. Their rationale is the fact that software add-ons can often create more issues than they solve and, in some cases, can increase the price of certain SaaS applications up to ten times.

Would you like to add additional granular access controls?

Password Management

Although passwords remain fundamental to IAM, many respondents are frustrated with their limitations and the effort that is involved in securing them at enterprise scale. Many have voiced the need to find alternatives to passwords and either management to contend with said limitations. With that being said, only 5% of respondents have implemented some form of passwordless controls, while 95% are using password-based controls.

Even amongst those who remain reliant on password-based controls, there is limited trust in today's solutions. As a result, many organizations are moving their credential storage to organization-owned repositories and prioritizing SSO integration over improvements in password management. Some PAM solutions manage who has access to what passwords, but they are often either too manual or too accessible to all employees. Using two-factor authentication mitigates this risk by integrating a password with another identification component.

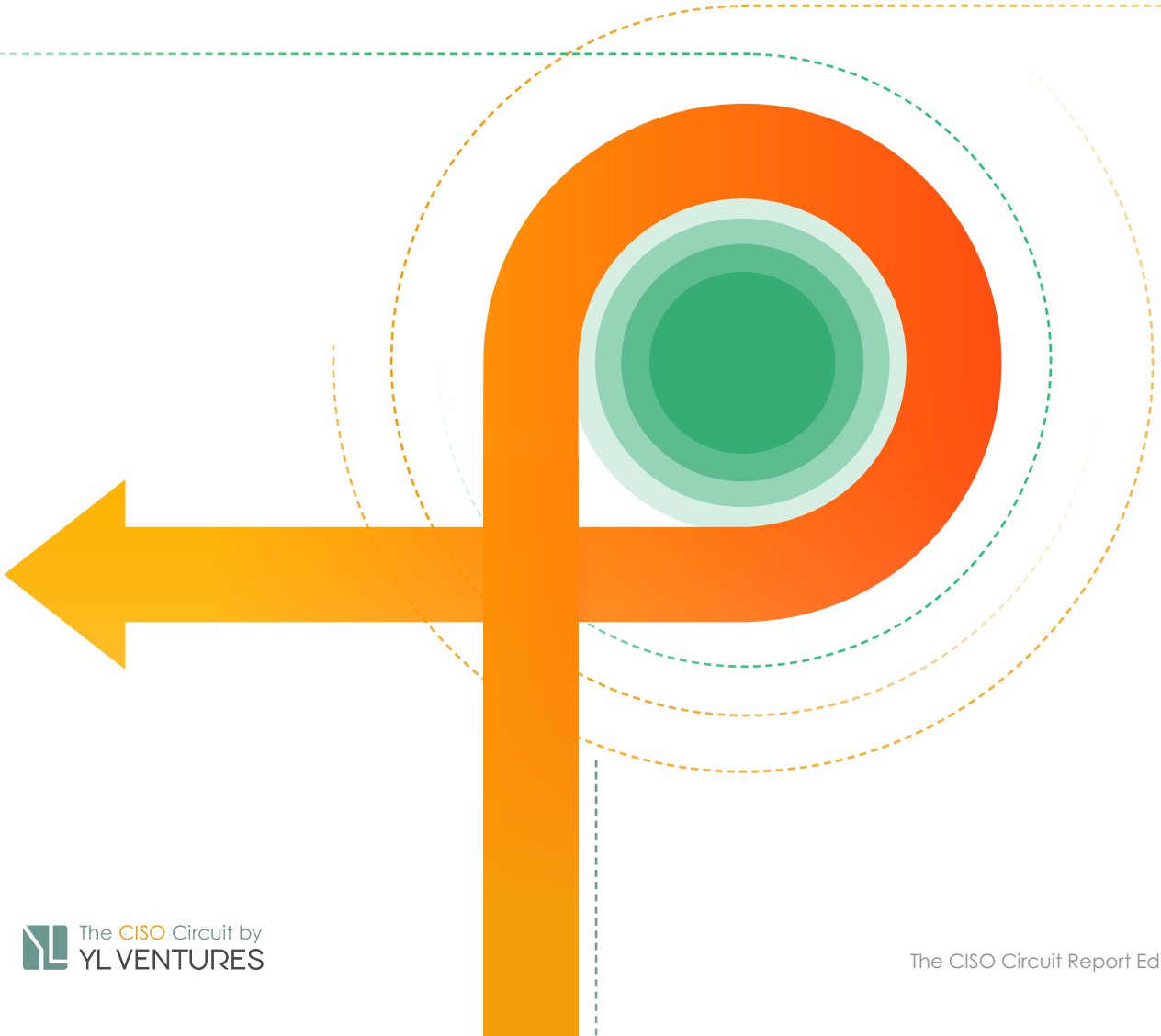
Are you currently using passwordless controls?

Final Observations

Traditional IAM is struggling to address the growing number and variety of identities that enterprise users today need to oversee and manage. This is compounded by the exponentially increasing amount of enterprise assets – applications, devices, infrastructure, to name a few – which various identities need access to. Part of this is due to the industry's traditional approach to identity and access, treating them as two separate fields instead of part of an integrated system. The resulting complex and disparate platforms have many security executives frustrated and in search of single-platform solutions that address all the issues without slowing down the speed of business.

However, within these struggles lie new opportunities. The enterprise IAM market is primed for solutions that can provide the kind of visibility and control over massive amounts and varieties of identities and assets. It further requires enhanced flexibility around the notion of identities and their behaviour, in light of today's workforce demands. Security across different types of identities – including users, applications and even devices – is needed, as are agile solutions that can adapt to remote and project-based work arrangements. As individuals increasingly require more access to various cloud infrastructures, SaaS applications and connected devices, enterprises must adapt to the growing number of assets they need to manage and provide access to.

A single source of truth which enables full management and visibility of identities and assets which identities need to access, is critical for the future of IAM providers. Early stage ventures would do well to innovate around providing overarching visibility and management, in order to align better with the challenges and realities faced by companies with modern and complex environments.



Outreach and Contact Information

This report was compiled with Israeli cybersecurity entrepreneurs in mind. If you are an Israeli-based start-up looking for guidance for seed-stage funding, we invite you to contact:

YL Ventures Partner & Head of Israel Office | Ofer Schreiber
ofer@ylventures.com

We would like to sincerely thank all of the CISOs that participated in this report. If you are an industry expert and would like to be interviewed for the next edition of the CISO Circuit, please contact:

YL Ventures Partner | John Brennan
john@ylventures.com

We also invite any questions relating to this report to be directed to:

YL Ventures Associate | Naama Ben Dov
naama@ylventures.com

Appendix

Survey Questions

1. What IAM (identity and access management) / IGA tools does your organization currently use?
2. Are you comfortable sharing which IAM/IGA vendors you use?
3. What difficulties are you currently experiencing with your IAM/IGA tools?
4. What new and/or emerging challenges are you experiencing in managing identity and access across your organization? What identity and/or access management products would you ideally have? For instance, has your expanding use of cloud infrastructure impacted your IAM needs?
5. What products and/or methodologies are you using to manage privileged identities and accounts? Are they sufficient? For instance, are they sufficient in cloud-native environments?
6. How are you managing developer access to production environments? Is this an important issue to you?
7. Have you centralized and/or automated access provisioning? Do you have different processes for provisioning access to different assets (e.g. different SaaS applications/cloud infrastructure)?
8. Would you buy a product that adds additional granular access controls to applications with coarse controls? If so, for which use cases? For instance, a product that generates additional roles in Slack.
9. How are you currently managing passwords, and what kind of challenges does this entail?